View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

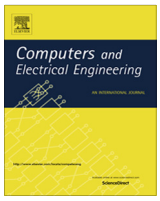
provided by Elsevier - Publisher Connector

Computers and Electrical Engineering 40 (2014) 539–550

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng



Analytical evaluation of a time- and energy-efficient security protocol for IP-enabled sensors ☆☆

Jasone Astorga *, Eduardo Jacob, Nerea Toledo, Marina Aguado

Department of Communications Engineering, University of the Basque Country UPV/EHU, Alameda de Urquijo s/n, 48013 Bilbao, Spain

ARTICLE INFO

Article history:
Available online 23 October 2013

ABSTRACT

With the development of the 6LoWPAN standard, sensors can be natively integrated into the IP world, becoming tiny information providers that are directly addressable by any Internet-connected party. To protect the information gathered by sensors from any potential attacker on the Internet, it is essential to have trustworthy real-time information about the legitimacy of every attempt to interact with a sensor. Our approach to address this issue is Ladon, a new security protocol specifically tailored to the characteristics of low capacity devices. In this paper, we study the performance of Ladon, showing that it successfully meets the requirements of the targeted environments. To that end, we evaluate the delay and energy consumption of the execution of Ladon. The obtained results show that the cost of Ladon is bounded, even in situations of high packet loss rates (20–80%) and comparable to that of other protocols that implement fewer security features.

© 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.

1. Introduction

Currently, the native integration of severely resource-deprived devices, such as sensors, in the IP world is already a reality. A key enabler of such environments is the 6LoWPAN approach [1], which aims to define how IP-based communications can be efficiently carried over IEEE 802.15.4 links. The fact that sensors become globally addressable in the Internet opens the door to the development and deployment of countless new applications, such as remote monitoring of patients [2] implanted with health sensors, in which any IP entity can establish an end-to-end communication with a sensor.

One of the most important hurdles to the widespread implementation of sensor-based applications is the protection of the information they manage. This issue entails the necessity of implementing security mechanisms that provide authentication and authorization of remote peers, as well as the necessity of ensuring the integrity and confidentiality of the transmitted information. This is complicated by the fact that typical sensors present severe constraints regarding processing power, storage and energy.

With the goal of providing resource-deprived devices with a suitable security protocol, we have developed Ladon [3], a novel security protocol that implements end-to-end authentication, authorization and key establishment functionalities at the application level. Taking into account the severe limitations of the environments for which Ladon has been designed, it is essential to prove its suitability. In this paper, we seek to carry out this proof with a detailed study regarding the impact of the execution of the Ladon protocol, based on an analytical model. Specifically, we evaluate two crucial performance parameters: the delay introduced by Ladon in establishing a secure connection and the energy consumed by the protected sensor as

☆☆ Reviews processed and recommended for publication to Editor-in-Chief by Associate Editor Dr. Jose Alcaraz Calero.

* Corresponding author. Tel.: +34 94 601 73 95.

E-mail addresses: jasone.astorga@ehu.es (J. Astorga), eduardo.jacob@ehu.es (E. Jacob), nerea.toledo@ehu.es (N. Toledo), marina.aguado@ehu.es (M. Aguado).

0045-7906 © 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
http://dx.doi.org/10.1016/j.compeleceng.2013.10.002

a result of implementing the security protocol. The obtained results show that the overhead introduced by the protocol is suitable for the targeted environments.

The rest of the paper is organized as follows. Section 2 provides a review on related work, while Section 3 provides information on preliminary concepts. Then, in Section 4 we describe the Ladon protocol and in Section 5, we present its performance evaluation. Finally, in Section 6, we highlight the most remarkable conclusions of our work.

2. Background and related work

The implementation of security mechanisms in sensor environments is a very active research area. Among the proposed approaches, there are initiatives aimed at the efficient implementation of cryptographic operations [4–7] and approaches focused on the efficient distribution of cryptographic keys [8–10]. Due to the severe limitations of the targeted environments, the developed protocols are each aimed at solving a specific issue. Therefore, they are very tightly linked to the characteristics of sensor networks and are not extensible to scenarios where access requests are originated outside such networks.

Regarding traditional security mechanisms, public key infrastructures are unsuitable for sensors, mainly due to the high resource consumption that they entail. With respect to mechanisms that solely make use of symmetric key cryptography, the Kerberos [11] protocol presents an interesting approach, mainly due to its centralized user account management. However, Kerberos does not address all of the security requirements presented by IP-enabled sensors, basically due to two reasons. First, Kerberos requires time synchronization, which implies the necessity of additional communication to periodically query time servers and which can render the protocol vulnerable to some security attacks. Second, Kerberos lacks authorization functionalities, which are essential in the considered scenarios.

For all of these reasons, the Ladon protocol [3] has been developed, based on the Kerberos architecture but tailored to the specific characteristics of resource-deprived devices. To the best of our knowledge, Ladon is the first protocol specifically designed to protect the data collected by sensors from illegitimate access originated by any entity connected to the Internet.

3. Preliminary concepts

3.1. Overview of Kerberos

Because Ladon is a protocol based on Kerberos, it is worth reminding some of the basic terminology and features of Kerberos. Each client or service is referred to as a *principal* in Kerberos, and each *principal* owns a secret key shared with the Kerberos Key Distribution Centre (KDC). The operation of Kerberos is based on the use of *tickets*, a capability distributed by the KDC that contains a proof of the identity of the principal that requested it.

Therefore, each client that wants to authenticate to a server needs a ticket issued by the Kerberos KDC for that service. To that aim, the client first authenticates against the Kerberos Authentication Server (AS) and obtains a long-term ticket known as a Ticket Granting Ticket (TGT). This ticket allows the client to securely communicate with the Kerberos Ticket Granting Server (TGS), which is in charge of issuing the actual Service Tickets. To avoid replay attacks, Kerberos includes timestamps in tickets and messages, requiring permanent clock synchronization among the interacting entities.

3.2. Comparison between Kerberos and Ladon

Ladon requires including two new information stores in the KDC: an *Active Connections Information Base*, to assess the freshness of tickets and messages, and an *Authorization Information Base*, to store authorization policies. Table 1 provides a concise comparison between Kerberos and Ladon.

4. Description of the Ladon protocol

This section provides a brief review of Ladon. Fig. 1 depicts the protocol operation and Table 2 details the contents of the exchanged messages. As shown in Fig. 1, Ladon entails three different phases: the authentication phase, the authorization phase and the service access phase, which are briefly described next. Readers desiring a more detailed description of Ladon are referred to [3], where a security validation of the protocol is also included.

Table 1
Comparison between Kerberos and Ladon.

	Kerberos	Ladon
Targeted protected devices	Powerful workstations	Severely resource-deprived devices
Authentication and key establishment functionality	✓	✓
Authorization functionality	×	✓
Independence of clock synchronization	×	✓

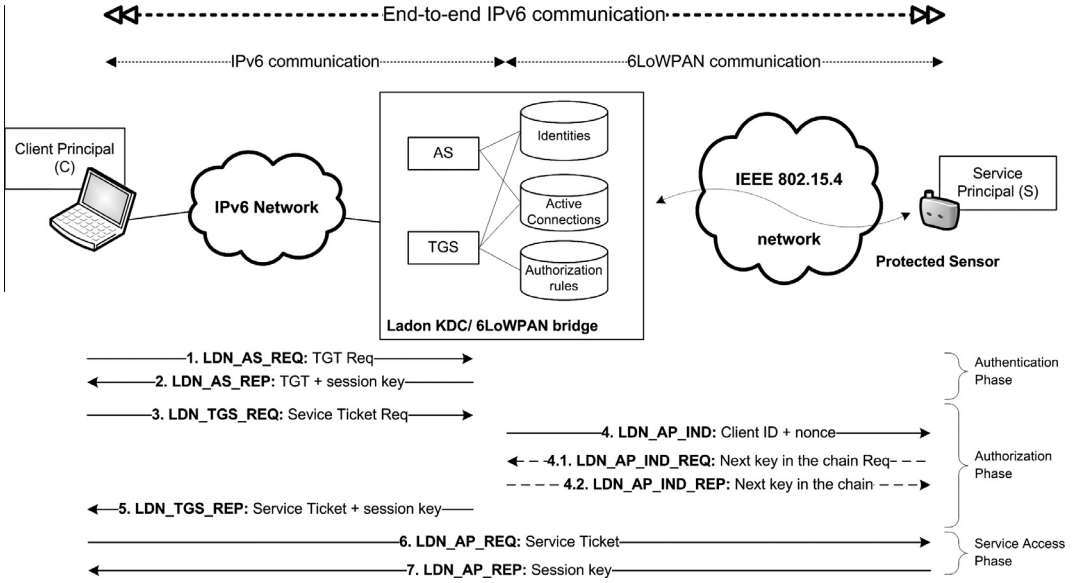


Fig. 1. Basic architecture and messages exchanged by the Ladon protocol.

Table 2
Detail of the content of Ladon messages.

Message	Direction	Content	
LDN_AS_REQ	$C \rightarrow AS$:	$ID_C \| ID_{TGS} \| Lifetime_1 \| Nonce_1$	
LDN_AS_REP	$AS \rightarrow C$:	$ID_C \| Ticket_{TGS} \| \{K_{C,TGS} \| Nonce_{C,TGS} \| Nonce_1 \| ID_{TGS}\}\ K_C$ $Ticket_{TGS} = \{K_{C,TGS} \| ID_C \| Nonce_{C,TGS}\}\ K_{TGS}$	*where*,
LDN_TGS_REQ	$C \rightarrow TGS$:	$ID_S \| Lifetime_2 \| Nonce_2 \| Ticket_{TGS} \| AuthN_{TGS}$ $AuthN_{TGS} = \{ID_C \|\| \ Nonce_{C,TGS} + i\}\ K_{C,TGS}$	*where*,
LDN_AP_IND	$TGS \rightarrow S$:	$ID_S \| ID_C \| Nonce_{C,S} \| Lifetime_2 \| K^i_{S,TGS} \| MAC(K_S, ID_C \| K^i_{S,TGS} \| Nonce_{C,S} \| Lifetime_2)$	
LDN_AP_IND_REQ	$S \rightarrow TGS$:	$ID_S \| Nonce_3 \| MAC(K_S, ID_S \| Nonce_3)$	
LDN_AP_IND_REP	$TGS \rightarrow S$:	$ID_S \| K^{i+1}_{S,TGS} \| MAC(K_S, ID_S \| Nonce_3 \| K^{i+1}_{S,TGS})$	
LDN_TGS_REP	$TGS \rightarrow C$:	$ID_C \| Ticket_S \| \{K_{C,S} \| Nonce_{C,S} \| Nonce_2 \| ID_S\}\ K_{C,TGS}$ $Ticket_S = \{K_{C,S} \| ID_C \| Nonce_{C,S} \| AuthZ\}\ K_S$ $AuthZ = \{RoleID\}\ K_S$	*where*,
LDN_AP_REQ	$C \rightarrow S$:	$Ticket_S \| AuthN_S \| Nonce_4$ $AuthN_S = \{ID_C \| Nonce_{C,S} \| Subkey\}\ K_{C,S}$	*where*,
LDN_AP_REP	$S \rightarrow C$:	$\{Nonce_{C,S} \| Subkey \| Nonce_4\} K_{C,S}$	

4.1. Security requirements of the Ladon protocol

The main goal of Ladon is to provide end-to-end authentication and authorization. However, several requirements specific to the characteristics of the targeted environments must also be addressed: energy efficiency, to maximize battery life; independence of clock synchronization, to avoid periodically querying time servers; support for multi-level access policies, to allow the enforcement of different access levels; resistance to message losses, to face protocol message losses; and centralized management of users and permissions, to allow the creation and enforcement of dynamic access policies without having to load them individually in each protected sensor.

4.2. Authentication phase

In the authentication phase, the client principal obtains a TGT that allows him to prove his identity to the Ladon TGS in order to obtain as many Service Tickets as he may need during the validity period of the TGT. To that aim, the client sends a LDN_AS_REQ message specifying his own identity (ID_C), and the Authentication Server responds with a LDN_AS_REP message conveying a new TGT and a new nonce value ($Nonce_{C,TGS}$), which is also stored in the Active Connections Information Base along with the client's identity. Associated with this entry, a lifetime is established with initial value $Lifetime_1$. After this lifetime expires, the entry is deleted, and thus the ticket containing the deleted nonce value is no longer valid. In this way, the possibility of old tickets being used as valid credentials is avoided.

4.3. Authorization phase

In the authorization phase, the client principal asks the TGS for a Service Ticket by means of a LDN_TGS_REQ message including the TGT obtained from the LDN_AS_REP message ($Ticket_{TGS}$). However, the TGT by itself is insufficient to authenticate a client, since TGTs can be resent. Therefore, an authenticator is used to prevent invalid replay of tickets.

After validating the received LDN_TGS_REQ message, the TGS verifies if the requesting client principal is authorized to access the desired service by querying the Authorization Information Base. This point constitutes an important difference with respect to Kerberos, where Service Tickets are provided to all authenticated principals. Next, the TGS sends a LDN_AP_IND message to the targeted service principal running on a sensor, specifying all of the information it will need afterwards to validate the LDN_AP_REQ request message. The service principal stores this information for a time $Lifetime_2$, and if the expected request from the client principal is not received before this time elapses, the service principal deletes the corresponding information in order to avoid overflowing the small storage capacity of the sensor.

An important aspect of Ladon is how LDN_AP_IND messages are authenticated. To this end, a mechanism based on one-way key functions is used. Each time the TGS sends a LDN_AP_IND message to a given service principal (S), it embeds a new value of a previously generated one-way key chain. The service principal, owning a value of the key chain $\left(K^{i-1}_{S,TGS}\right)$, cannot calculate the next value $\left(K^{i}_{S,TGS}\right)$, due to the characteristics of one-way functions. However, it can authenticate the received LDN_AP_IND message by checking that $F\left(K^{i}_{S,TGS}\right) = K^{i-1}_{S,TGS}$. To provide each service principal with the first value of the key chain, the LDN_AP_IND_REQ/_REP exchange is used.

Lastly, the TGS responds to the client with a LDN_TGS_REP message including the requested Service Ticket ($Ticket_S$).

4.4. Service access phase

In the service access phase, the client principal requests access to the data provided by the sensor through a LDN_AP_REQ message. This message includes the previously obtained Service Ticket, which identifies the client as an authenticated and authorized party. The service principal validates the LDN_AP_REQ message using the information provided by the TGS in the LDN_AP_IND message. After a positive validation, the service principal responds to the client with a LDN_AP_REP message either accepting the key proposed in the request message (*subkey*) or proposing a new one. This key can be used afterwards to derive further encryption and integrity keys.

4.5. Recovery mechanisms

As wireless links are prone to packet losses, it is essential to implement efficient recovery mechanisms. For the exchanges started by the LDN_AS_REQ, LDN_TGS_REQ, LDN_AP_REQ and LDN_AP_IND_REQ request messages, the designed recovery mechanisms consist in retransmitting the given request if the expected response does not arrive within a predefined time frame.

However, this mechanism is not valid for LDN_AP_IND messages, because they lack an associated response. The mechanism used in this case relies on the properties of one-way functions and is more efficient than any procedure involving message retransmissions. The service principal successively applies the one-way function to the received $K^{j}_{S,TGS}$ value, and if any of the obtained results coincide with its stored value, the server accepts the message and stores the received $K^{j}_{S,TGS}$ value. However, if after the maximum number of attempts to compute the one-way function, the service principal is still unable to validate the received $K^{j}_{S,TGS}$ value, a more expensive mechanism must be used, consisting of the LDN_AP_IND_REQ/_REP exchange.

5. Performance evaluation: time and energy consumption

In this section, we detail the performance evaluation of our protocol, demonstrating its applicability to the targeted sensor devices. To this end, we evaluate the delay introduced by the protocol for the establishment of a secure connection and the energy consumed by the sensor during this process.

5.1. Modelled scenario and assumptions

For our study, we consider a beacon-enabled cluster-tree structure of the IEEE 802.15.4 network. In the envisioned topology, there is a PAN coordinator with three sub-coordinators, and each sub-coordinator has three child coordinators. Each cluster consists of 6 sensor devices with a service principal running in each sensor. Therefore, a total of 54 service principals exist in the network, with a 3-hop depth from the PAN coordinator to any of the service principals. Fig. 2 represents a single branch of the considered IEEE 802.15.4 network. The other two identical branches have been omitted.

For the sake of simplicity, we omit the authentication phase, because it is only performed once during the validity lifetime of the TGT and does not involve any resource-deprived device. Additionally, for the computation of end-to-end transmission delays only the delays introduced by the IEEE 802.15.4 network have been considered, as the delay introduced by the Internet connection is commonly orders of magnitude smaller.

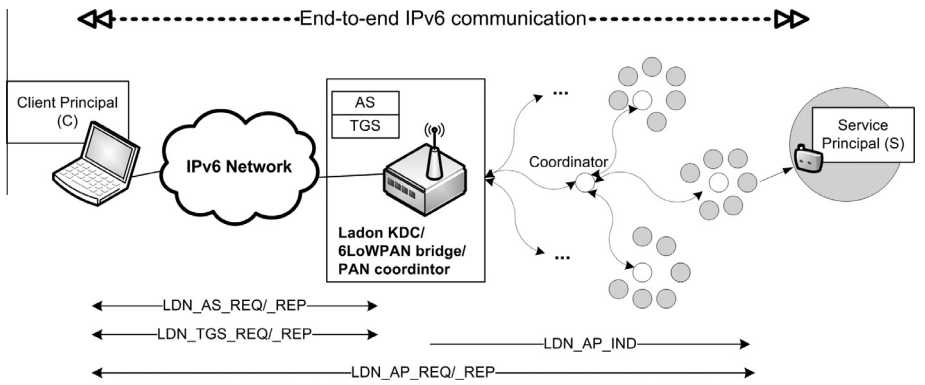


Fig. 2. Topology of the considered network scenario.

5.2. End-to-end secure session establishment delay

Fig. 3 shows the different time intervals that affect the establishment of a secure connection. As can be seen in the figure, each message entails a generation time (S_{Xi}), a transmission time (t_{ni}), a queue waiting time in the destination entity (W_{Xi}) and a processing time (S_{Xi}). Therefore, the delay to establish a secure session can be represented in the following way:

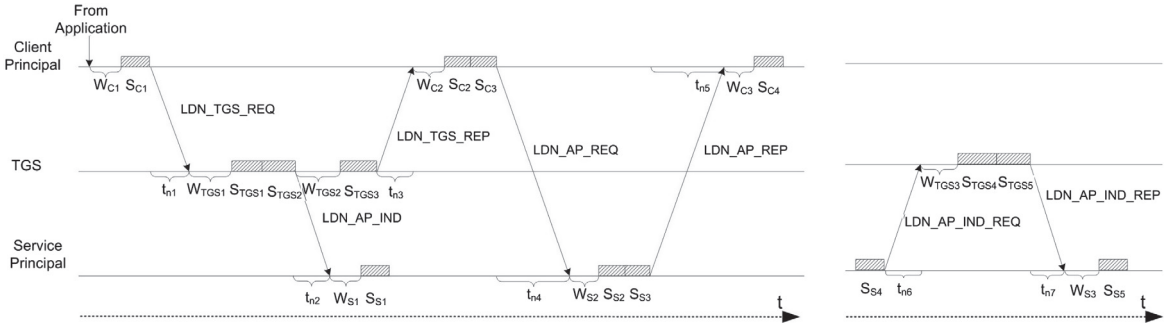
$$D_{SS} = (R_1+1)(E[W_{C1}] + S_{C1} + t_{n1} + E[W_{TGS1}] + S_{TGS1} + S_{TGS2} + W_{TGS2} + S_{TGS3} + t_{n3} + E[W_{C2}] + S_{C2}) + (R_2+1)(S_{C3} + t_{n4} + E[W_{S2}] + S_{S2} + S_{S3} + t_{n5} + E[W_{C3}] + S_{C4}) + \left(\frac{1}{L} + \frac{L-1}{L}P_L^Q\right)(R_3+1)(S_{S4} + t_{n6} + E[W_{TGS3}] + S_{TGS4} + S_{TGS5} + t_{n7} + E[W_{S3}] + S_{S5}) \quad (1)$$

where $E[W_X]$ denotes the expectation of the W_X queue waiting time, P_L represents the packet loss probability in the IEEE 802.15.4 network, L denotes the length of the one-way key chain and Q denotes the maximum number of attempts to successively execute the one-way function. Additionally, R_1, R_2 and R_3 represent the expected number of LDN_TGS_REQ, LDN_AP_REQ and LDN_AP_IND_REQ retransmission attempts, respectively. These values are calculated in the Appendix. From Eq. (A.1), we conclude that $R_1 \simeq 0$. That is, LDN_TGS_REQ messages are not retransmitted.

In the considered context, it is reasonable to assume that all of the messages received by the client principal spend the same average time waiting to be served ($E[W_C]$). The same happens in the service principal ($E[W_S]$). However, in the case of the TGS, W_{TGS2} takes a fixed value different from $E[W_{TGS1}]$ and $E[W_{TGS3}]$, because W_{TGS2} is a fixed guard interval used to ensure that the LDN_AP_REQ message does not arrive at the service principal until the corresponding LDN_AP_IND has been received and processed.

Therefore, to calculate W_{TGS2}, we consider the worst case scenario, in which the LDN_AP_IND message arrives at the service principal after the last allowed retransmission attempt (K) and cannot be implicitly authenticated after Q executions of the one-way function, and the LDN_AP_IND_REQ is retransmitted for the maximum allowed attempts (M).

$$W_{TGS2} \geqslant t_{n2} + E[W_S] + K(E[W_{TGS}] + S_{TGS2} + t_{n2} + E[W_S]) + S_{S1}|Qattempts + (M+1)(E[W_S] + S_{S4} + t_{n6} + E[W_{TGS}] + S_{TGS4} + S_{TGS5} + t_{n7} + E[W_S] + S_{S5}) - E[W_S] - S_{TGS3} - t_{n3} - E[W_C] - S_{C2} - S_{C3} - t_{n4} - E[W_S] \quad (2)$$



(a) Message exchange during the normal operation of Ladon

(b) Message exchange LDN_AP_IND_REQ/_REP

Fig. 3. Time sequence of the establishment of a Ladon secure connection.

5.2.1. Service time analysis

To calculate the service times corresponding to the processing or generation of messages, we consider constant rates for the execution of cryptographic operations in each entity. We therefore calculate the S_{Xi} parameters of Eq. (1) as:

$$S_{Xi} = \frac{|CRYP(Message)|}{TCRYP_X} \tag{3}$$

where $|CRYP(Message)|$ denotes the length of the fields to be cryptographically processed and $TCRYP_X$ denotes the cryptographic operations execution rate of entity X. Table 3 summarises the lengths of Ladon protocol messages, along with the number of bytes that are subject to cryptographic operations in each entity. These figures have been computed assuming 16-byte cryptographic keys, 8-byte nonces and 2-byte identity fields.

5.2.2. Transmission time analysis

To compute the transmission times (t_{ni} values in Eq. (1)), we consider the delays introduced by the three wireless hops of the IEEE 802.15.4 network, including a backoff time (D_{BOT}) and a data transmission time (D_{Tx}):

$$t_{ni} = \sum_{l=1}^{3} D_{BOT}^{l} + D_{Tx}^{l} \tag{4}$$

To calculate the backoff time, we follow the model proposed in [12]. We first calculate the probability (q) that a transmission of a given type of Ladon message is detected by Clear Channel Assessment (CCA) during the Contention Access Period (CAP) as a function of the message length, the CAP length (t_{CAP}) and the data rate of the wireless link (R). We then calculate the average amount of data transmitted during CAP (d) for each coordinator. As an example, Eqs. (5) and (6) represent the q and d values corresponding to the LDN_AP_IND messages routed by the PAN coordinator (C_0):

$$q_{AP\_IND} = \frac{|LDN\_AP\_IND|}{t_{CAP}R} \tag{5}$$

$$d_{AP\_IND}^{C_0} = \lambda_0 N_S N_C E[LDN\_AP\_IND] t_{CAP} \tag{6}$$

Here $|LDN\_AP\_IND|$ denotes the length of the LDN_AP_IND message and $E[LDN\_AP\_IND]$ as calculated in Eq. (A.2). Additionally, N_C and N_S represent the number of clients and servers in the network, respectively, and λ_0 denotes the average rate at which each client generates access requests to each server. Therefore, the probability of detecting a clear channel by CCA (p_c) is independently calculated for each coordinator:

$$p_c^{C_0} = (1 - q_{AP\_IND})^{d_{AP\_IND}^{C_0}(1-h)} \times (1 - q_{AP\_IND\_REQ})^{d_{AP\_IND\_REQ}^{C_0}(1-h)} \times (1 - q_{AP\_IND\_REP})^{d_{AP\_IND\_REP}^{C_0}(1-h)} \times (1 - q_{AP\_REQ})^{d_{AP\_REQ}^{C_0}(1-h)} \times (1 - q_{AP\_REP})^{d_{AP\_REP}^{C_0}(1-h)} \tag{7}$$

where h represents the probability that two randomly deployed nodes in the coverage range of a given coordinator have a hidden node relationship.

If the CCA is unsuccessful, the backoff algorithm is repeated up to a maximum of b attempts. The probability of a successful CCA (s) and the average number of backoff attempts (r) are calculated in the following way:

$$s^{C_0} = \sum_{a=1}^{b} p_c^{C_0} \left(1 - p_c^{C_0}\right)^{(a-1)} \tag{8}$$

$$r^{C_0} = (1 - s^{C_0})b + \sum_{a=1}^{b} a p_c^{C_0} \left(1 - p_c^{C_0}\right)^{(a-1)} \tag{9}$$

Table 3
Lengths of Ladon protocol messages and the number of bytes over which each entity must perform cryptographic operations.

Message type	Length (bytes)	Bytes subject to cryptographic operations		
		Client principal (bytes)	KDC (bytes)	Service principal (bytes)
LDN_AS_REQ	15	–	–	–
LDN_AS_REP	62	34	60	–
LDN_TGS_REQ	47	10	36	–
LDN_AP_IND	33	–	27	27
LDN_AP_IND_REQ	14	–	10	10
LDN_AP_IND_REP	22	–	26	26
LDN_TGS_REP	63	34	62	–
LDN_AP_REQ	61	26	–	54
LDN_AP_REP	32	32	–	32

Then, the total backoff time in each coordinator is calculated as follows:

$$t_{BOT}^{C_0} = \frac{3}{2} r^{C_0}(t_{IR} + t_{CCA}) + \sum_{a=0}^{r^{C_0}-1} t_{BO}(min(macMinBE + a, aMaxBE)) \tag{10}$$

where t_{IR} is the idle to receive transition time, t_{CCA} is the CCA analysis time and $t_{BO}(BE)$ is given by Eq. (11), where t_{BOP} is the backoff length.

$$t_{BO}(BE) = \frac{2^{BE} - 1}{2} t_{BOP} \tag{11}$$

Lastly, the actual transmission time of each message is calculated considering a constant transmission rate for the IEEE 802.15.4 wireless link (R).

5.2.3. Waiting time analysis

We model the three entities (client and service principals and TGS) as M/G/1 queues, because they process variable length messages and thus the service times can be represented with a general distribution. As before, we consider N_C clients generating requests according to a Poisson distribution with mean rate λ_0 to the each of the N_S servers in the network. The mean arrival rates of jobs (λ) to each entity are expressed as:

$$\lambda_C = 3N_S\lambda_0 + (R_2 + 1)N_S\lambda_0 \tag{12}$$

$$\lambda_{TGS} = N_S N_C \lambda_0 \left[2 + \frac{(L-1)}{L} + \frac{1}{L}(R_4 + 1) + \frac{1}{L}(1 - P_L)(R_3 + 1) + \frac{(L-1)}{L} P_L^Q (1 - P_L)(R_3 + 1)\right] \tag{13}$$

$$\lambda_S = N_C \lambda_0 \left\{ \left[\frac{(L-1)}{L} + \frac{1}{L}(R_4 + 1)\right](1 - P_L) + (1 - P_L)(R_2 + 1) + \left(\frac{1}{L} + \frac{(L-1)}{L} P_L^Q\right)[(R_3 + 1) + 1]\right\} \tag{14}$$

Similarly, for each entity we calculate the average service time ($\overline{X}$) as follows:

$$\overline{X_C} = \frac{S_{C1} + S_{C2} + S_{C3} + S_{C4}(R_2 + 1)}{3 + (R_2 + 1)} \tag{15}$$

$$\overline{X_{TGS}} = \frac{S_{TGS1} + S_{TGS2}\left[\frac{L-1}{L} + \frac{1}{L}(R_4 + 1)\right] + S_{TGS3}}{2 + \frac{L-1}{L} + \frac{1}{L}(R_4 + 1) + \left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)(1 - P_L)(R_3 + 1)} + \frac{S_{TGS4}\left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)(1 - P_L)(R_3 + 1)}{2 + \frac{L-1}{L} + \frac{1}{L}(R_4 + 1) + \left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)(1 - P_L)(R_3 + 1)} \tag{16}$$

$$\begin{aligned}\overline{X_S} = {} & \frac{E[S_{S1}]\left[\frac{L-1}{L} + \frac{1}{L}(R_4 + 1)\right](1 - P_L) + (S_{S2} + S_{S3})(1 - P_L)(R_2 + 1)}{\frac{L-1}{L} + \left[\frac{1}{L}(R_4 + 1) + (R_2 + 1)\right](1 - P_L) + \left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)[(R_3 + 1) + 1]} \\ & + \frac{S_{S4}\left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)(R_3 + 1) + S_{S5}\left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)}{\frac{L-1}{L} + \left[\frac{1}{L}(R_4 + 1) + (R_2 + 1)\right](1 - P_L) + \left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)[(R_3 + 1) + 1]}\end{aligned} \tag{17}$$

Lastly, the average waiting time in queue for each entity (X) is the following:

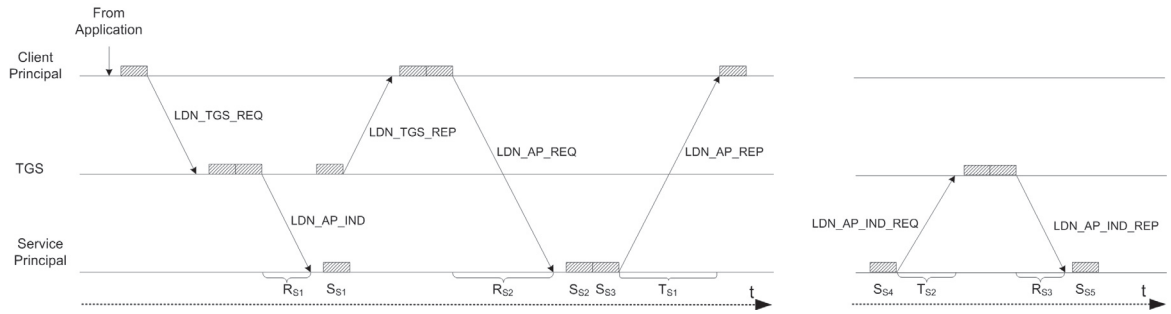
$$E[W_X] = \frac{\lambda_X \overline{X_X^2}}{2(1 - \rho_X)} \tag{18}$$

where $\rho_X = \lambda_X \overline{X_X}$ denotes the server utilization.

5.3. Energy consumption

To evaluate the energy consumed by a sensor to establish a secure connection, we take into account the energy consumed by transmission and reception of bits over the air, as well as by the execution of cryptographic operations. Fig. 4 represents the Ladon message exchanges, indicating the operations that imply energy consumption in the protected sensor. Therefore, the total amount of energy consumed for establishing a secure session is the following:

$$\begin{aligned}\varepsilon_{SS} = {} & \left[\frac{L-1}{L} + \frac{1}{L} E[LDN\_AP\_IND]\right](1 - P_L) R_{S1} + \left[\frac{L-1}{L} + \frac{1}{L} E[LDN\_AP\_IND]\right] \\ & (1 - P_L)\left[S_{S1} + E[Hash] + \left(\frac{1}{L} + \frac{L-1}{L} P_L^Q\right)[E[LDN\_AP\_IND\_REQ](S_{S4} + T_{S2}) + R_{S3} + S_{S5}]\right] \\ & + E[LDN\_AP\_REQ](1 - P_L)(R_{S2} + S_{S2} + S_{S3} + T_{S1})\end{aligned} \tag{19}$$



(a) Message exchange during the normal operation of Ladon

(b) Message exchange LDN_AP_IND_REQ/_REP

Fig. 4. Causes of energy consumption in a protected service principal.

$$E[Hash] = \frac{L-1}{L}\left(1-P_L^Q\right)\frac{(1-P_L^Q)-QP_L^Q(1-P_L)}{(1-P_L)}H + \left(\frac{1}{L}+\frac{L-1}{L}P_L^Q\right)QH \tag{20}$$

being H the energy consumed by one execution of the one-way function.

To calculate the average energy consumed due to the transmission and reception of bits, we take into account the length of Ladon messages as gathered in Table 3, a constant transmission rate (R) and independent instantaneous power consumptions for the reception (P_{RX}) and transmission (P_{TX}) operations. In the case of the transmission operations, we also consider the energy consumed during the backoff process, which is calculated as in [12].

Similarly, to calculate the energy consumed during cryptographic processing, we assume constant bit rates and consider constant instantaneous power consumption (P_C) during the execution of such operations.

5.4. Results and discussion

We use Eqs. (1) and (19) to evaluate the mean delay and energy consumption of a secure session establishment as functions of the packet loss probability in the IEEE 802.15.4 network. For the sake of obtaining numerical results, we use the parameterisation summarized in Tables 4–6.

As shown in Fig. 5a and b, the time needed for a secure session establishment is bounded and within an acceptable limit even for high packet loss situations in which the different protocol messages are retransmitted multiple times. The same result is found for the amount of energy consumed by the protected sensor devices. In the case of very high packet loss probabilities, very few of the transmitted messages arrive at their destination and therefore, the energy consumed by the protected sensors is drastically reduced, because they do not expend energy in the corresponding reception and processing operations or in the transmission of the associated response messages. Additionally, the average delay does not tend to infinity because the number of retransmissions of each type of message is bounded. In such cases, the probability that the secure session is successfully established is very small.

With the objective of comparing Ladon with similar approaches, we have modelled Kerberos and the SPINS-based key exchange protocol presented in [6], as they are the closest ones to Ladon in terms of functionality. Specifically, the SPINS-based protocol relies on using the base station as a trusted third party so that two sensors within the same network can agree

Table 4
Parameters used for the performance analysis and their values.

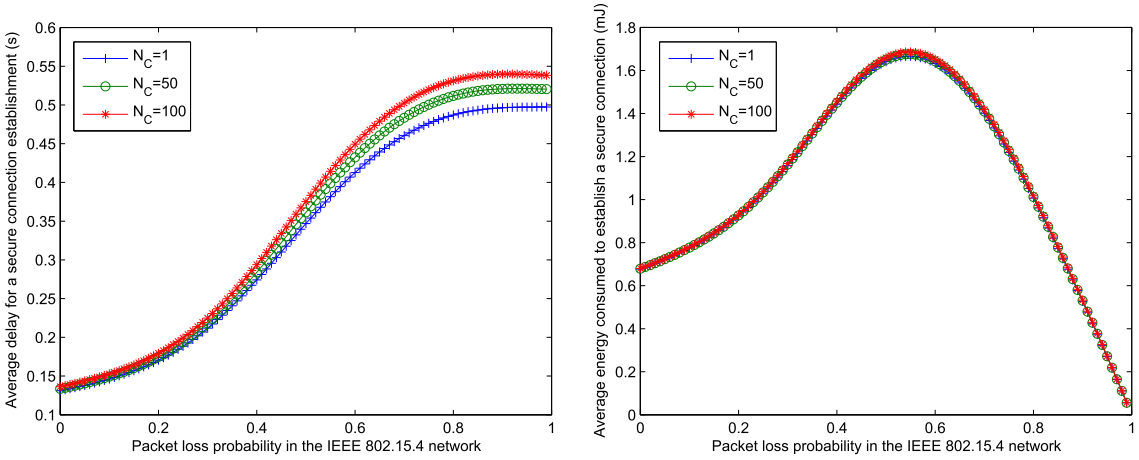
Parameter	Description	Value
L	Length of the one-way key chain	100
Q	Maximum number of one-way function execution attempts	10
W	Maximum number of retransmissions of LDN_TGS_REQ messages	1
K	Maximum number of retransmissions of LDN_AP_IND messages	2
M	Maximum number of retransmissions of LDN_AP_IND_REQ messages	1
V	Maximum number of retransmissions of LDN_AP_REQ messages	8
$TCRYP_C$	Cryptographic operations performance rate of the client principal	1 Mbps
$TCRYP_S$	Cryptographic operations performance rate of the service principal	50 Kbps
$TCRYP_{TGS}$	Cryptographic operations performance rate of the TGS	2 Mbps
λ_0	Job generation rate of each client principal	1 request/min
N_S	Number of service principals	54

Table 5
Parameters used for modelling IEEE 802.15.4 links.

Name	Description	Value
t_{CAP}	Duration of the CAP period	61.44 ms
R	Wireless link data rate	250 Kbps
h	Hidden node relationship probability	41%
b	Maximum number of backoff attempts	4
t_{IR}	Idle to receive transition time	192 μs
t_{CCA}	CCA analysis time	128 μs
macMinBE	Initial value of the backoff exponent	3
aMaxBE	Maximum value of the backoff exponent	5
t_{BOP}	Backoff period length	320 μs

Table 6
Characterization of energy consumption in sensor nodes.

Name	Description	Processor mode	Radio mode	Value (mW)
P_{RX}	Power consumption in reception mode	Active	Rx	74.4
P_{TX}	Power consumption in transmission mode	Active	Tx (0dBm)	65.7
P_C	Power consumption in cryptographic processing mode	Active	Idle	5.4



(a) Average delay to establish a Ladon secure session

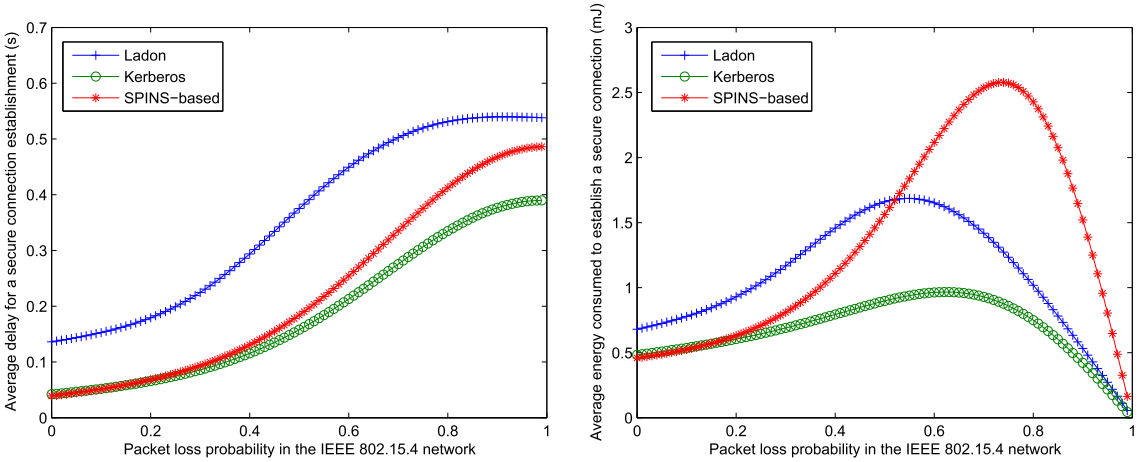
(b) Average energy consumed to establish a Ladon secure session

Fig. 5. Analysis of the energy and time consumed to establish a Ladon secure session.

upon a shared key. We have chosen this protocol for the comparison because out of the key exchange protocols specifically designed for sensor networks, it is the most easily extensible to more generalist scenarios.

The scenario considered for the comparison corresponds to the most demanding of the previously evaluated situations: 100 clients sending requests at an average rate of $\lambda_0 = 1\, requests/min$. The results gathered in Fig. 6a show that the time needed to establish a secure session using Ladon is longer than the time needed by the other two evaluated protocols. However, this time is still limited and is acceptable for the considered scenarios. As an example, for a wide range of packet loss probabilities, the delay introduced by Ladon is lower than the maximum allowed response time for a web server [13]. In this sense, it must be remarked that Ladon provides additional authorization functionality, while the other two compared protocols do not.

On the other hand, Fig. 6b shows that in an ideal situation ($P_L = 0$), the energy consumed by Ladon is slightly higher than the energy consumed by the other two protocols but is in a comparable range. If packet losses occur, which is a common situation in sensor networks, the energy consumption of Ladon becomes similar to the energy consumed by Kerberos and lower than the energy consumed by the protocol introduced in [6]. Fig. 6b shows that for common packet loss rates in sensor networks (20–80%) [14], Ladon consumes about 15% less energy than the SPINS-based protocol. We therefore demonstrate



(a) Average time consumed by different protocols to establish a secure session

(b) Average energy consumed by different protocols to establish a secure session

Fig. 6. Analysis of the time and energy consumed by different protocols to establish a secure session.

that in a real situation, Ladon outperforms alternative key establishment protocols specifically designed for sensor environments.

6. Conclusions

We have presented the security needs that must be addressed before sensors can be securely integrated into the IP world. As a suitable alternative to address these needs, we propose Ladon, a protocol based on Kerberos but specifically tailored to the requirements of sensor environments. We have evaluated the time and energy overhead introduced by Ladon when establishing a secure connection. The obtained results demonstrate that the protocol is well tailored to the requirements of the targeted resource-deprived environments in real network situations, i.e., in situations where the packet losses in the network are frequent.

We lastly have compared the performance of Ladon with that of protocols that implement even more limited characteristics (they lack authorization mechanisms), such as Kerberos and a protocol based on SPINS. Although Ladon introduces a longer delay than the other two protocols, the difference is negligible for the application context considered for our protocol. Regarding energy consumption, the obtained results show that it is comparable for the three evaluated protocols, and in cases of high packet loss probability, the amount of energy consumed by Ladon is lower than the energy consumed by the protocol based on SPINS. This fact proves that Ladon deals more efficiently with packet losses in the network.

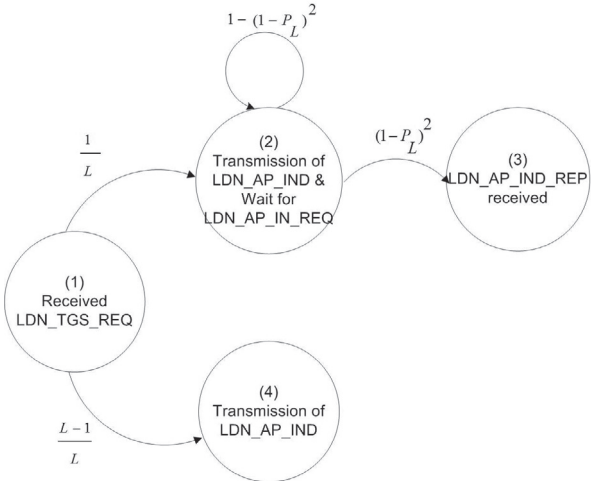
In conclusion, we have demonstrated that Ladon is a time- and energy-efficient solution and is thus feasible for addressing security in targeted resource-deprived environments.

Appendix A. State transition modelling

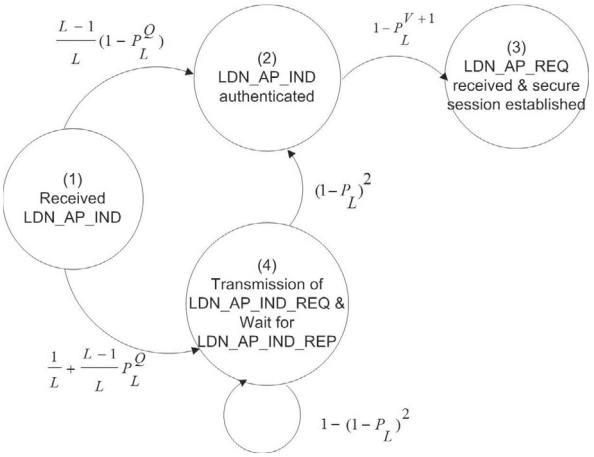
Fig. A depicts the state transition models of the participating entities, where P_L denotes the packet loss probability in the IEEE 802.15.4 network, Y, W, V, K and M denote the maximum allowed number of retransmissions for LDN_AS_REQ, LDN_TGS_REQ, LDN_AP_REQ, LDN_AP_IND and LDN_AP_IND_REQ messages, respectively, and L represents the length of the one-way key chain. We next calculate the average number of transmission attempts of each request message assuming that each occurrence of loss of a given type of message is random and mutually independent.

$$E[LDN\_TGS\_REQ] = R_1 + 1 = \sum_{k=1}^{W+1} kP(I=k) = \sum_{k=1}^{W} k\left[1 - \frac{[1-(1-P_L)^2]^{K+1}}{L}\right]\left[\frac{[1-(1-P_L)^2]^{K+1}}{L}\right]^{k-1} + (W+1)\left[1 - \sum_{k=1}^{W}\left[1 - \frac{[1-(1-P_L)^2]^{K+1}}{L}\right]\left[\frac{[1-(1-P_L)^2]^{K+1}}{L}\right]^{k-1}\right] \quad (A.1)$$

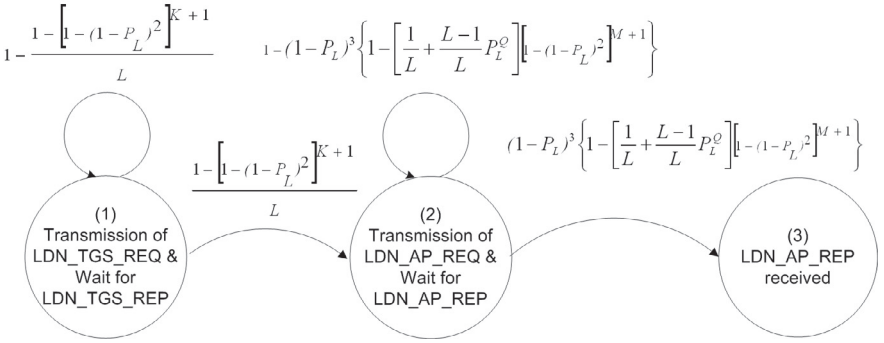
$$E[LDN\_AP\_IND] = \sum_{k=1}^{K+1} kP(I=k) = \sum_{k=1}^{K} k(1-P_L)^2[1-(1-P_L)^2]^{k-1} + (K+1)\left[1 - \sum_{k=1}^{K}(1-P_L)^2[1-(1-P_L)^2]^{k-1}\right] \quad (A.2)$$



(a) State transition diagram of the TGS



(b) State transition diagram of the service principal



(c) State transition diagram of the client principal

Fig. A. State transition models of the TGS, service principal and client principal.

$$E[LDN\_AP\_IND\_REQ] = R_3 + 1 = \sum_{k=1}^{M+1} kP(I=k) = \sum_{k=1}^{M} k(1-P_L)^2\left[1-(1-P_L)^2\right]^{k-1} + (M+1)\left[1-\sum_{k=1}^{M}(1-P_L)^2\left[1-(1-P_L)^2\right]^{k-1}\right] \tag{A.3}$$

$$E[LDN\_AP\_REQ] = R_2 + 1 = \sum_{k=1}^{V+1} kP(I=k) = (1-P_L)^3 R\sum_{k=1}^{V} k\left[1-(1-P_L)^3 R\right]^{k-1} + (V+1)\left[1-(1-P_L)^3 R\sum_{k=1}^{V}\left[1-(1-P_L)^3 R\right]^{k-1}\right]$$
$$being, R = 1-\left[1-(1-P_L)^2\right]^{M+1}\left[\frac{1}{L}+\frac{(L-1)}{L}P_L^Q\right] \tag{A.4}$$

References

[1] Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 packets over IEEE 802.15.4 networks. Tech. Rep. 4944; September 2007.
[2] Gupta R, Bera J, Mitra M. A bi-phase enabled serial acquisition system for remote processing of digitized ECG. Comput Electr Eng 2012;38(1):68–74.
[3] Astorga J, Jacob E, Huarte M, Higuero M. Ladon: end-to-end authorisation support for resource-deprived environments. IET Inf Secur 2012;6(2):93–101.
[4] Efstathiou C, Moschopoulos N, Voyiatzis I, Pekmestzi K. On the design of modulo $2n + 1$ dot product and generalized multiply-add units. Comput Electr Eng 2013;39(2):410–9.

[5] Kitsos P, Sklavos N, Parousi M, Skodras AN. A comparative study of hardware architectures for lightweight block ciphers. Comput Electr Eng 2012;38(1):148–60.
[6] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. SPINS: security protocols for sensor networks. Wirel Net 2002;8(5):521–34.
[7] Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks. In: Proc. 2nd intl conf on embedded networked sensor systems, SenSys'04. New York, NY, USA: ACM; 2004. p. 162–75.
[8] Zhu S, Setia S, Jajodia S. LEAP: efficient security mechanisms for large-scale distributed sensor networks. In: Proc 10th ACM conf on computer and communications security, CCS'03. New York, NY, USA: ACM; 2003. p. 62–72.
[9] Chan H, Perrig A. PIKE: peer intermediaries for key establishment in sensor networks. In: Proc 24th annual joint conf of the IEEE computer and communications societies, INFOCOM'05; 2005. p. 524–35.
[10] Watro R, Kong D, fen Cuti S, Gardiner C, Lynn C, Kruus P. TinyPK: securing sensor networks with public key technology. In: Proc 2nd ACM workshop on security of ad hoc and sensor networks, SASN'04. New York, NY, USA: ACM; 2004. p. 59–64.
[11] Neuman C, Yu T, Hartman S, Raeburn K. The Kerberos network authentication service (V5). Tech. Rep. 4120; July 2005.
[12] Kohvakka M, Kuorilehto M, Hännikäinen M, Hämäläinen TD. Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications. In: Proc 3rd ACM intl workshop on performance evaluation of wireless ad hoc, sensor and ubiquitous networks, PE-WASUN'06. New York, NY, USA: ACM; 2006. p. 48–57.
[13] Nielsen J. Usability engineering. Morgan Kaufmann, San Francisco, USA; 1993.
[14] Shu F, Sakurai T, Zukerman M, Vu H. Packet loss analysis of the IEEE 802.15.4 MAC without acknowledgements. IEEE Commun Lett 2007;11(1):79–81.

Jasone Astorga received her Ph.D. and M.Sc. degrees in Telecommunication Engineering from the University of the Basque Country (UPV/EHU). From 2004 to 2007 she worked in Nextel S.A., a Telecommunications enterprise. From 2007 she works as lecturer and researcher in I2T Research Lab at the UPV/EHU. Her research interests include wireless networking, IP-enabled sensors, security and mobility management.

Eduardo Jacob received his M.Sc. in Industrial Communications and Electronics and Ph.D. in ICT from the University of the Basque Country. He is assistant professor and Head of the Communications Engineering Department of the same university and leads the I2T Research Lab. His research interests are related to Software Defined Networks, communications security and IP-enabled wireless sensors.

Nerea Toledo received her Ph.D. and M.Sc. degrees in Telecommunication Engineering both from the University of The Basque Country. She works as an assistant professor and as a researcher in I2T Research Lab in the same university. Her research interests include wireless networking, mobility management, security applied to the ITS scenario, and wireless sensor networks.

Marina Aguado is Associate Professor at the University of The Basque Country and Senior Researcher in I2T Research Lab at the same university. Her expertise focuses in communication technologies for transport systems with eight years experience in the railway transportation industry, having held various positions, from R&D Manager, Consultant, Project Manager and Network Support Analyst.